CLAIMS

We claim:

1. a method for the delivery and use of electronic media, characterised by:
   a) Parts of the media being distributed for a client in a disabled form.
   b) A media enabling mechanism being provided for the client through a communications network.
   c) A Client Instantiation Component (CIC) instantiating or otherwise enabling the use of the media parts.

2. A method in accordance with claim1, wherein selected components on the client machine are optionally secured before the media enabling mechanism is provided to the client.

3. A method in accordance with claim 2, wherein said component securing is performed by one or more of the following securing mechanisms:
   a) Calculating a hash function for selected components. Said hash function results ideally being returned to a networked machine for validation.
   b) Delivering and using fresh secure components.
   c) The use of private and public key certificates to sign the components.
   d) Using hardware or ROM implementations of the secured components.

4. A method in accordance with claims 2 and 3, wherein the securing mechanism is itself secured by means of a known identifier, trusted connection or other means and may optionally have to return information to a networked machine or component within a time-limit.

5. A method in accordance with claims 2, 3 or 4 wherein the securing mechanism is a Checking Module distributed to the client from a networked machine over a communications medium.

6. A method in accordance with any of the previous claims wherein components accessible by the client are automatically replaced if they are judged insecure or outdated.

7. A method in accordance with any of the previous claims wherein the disabled media parts are disabled by one or more of the following:
   a) Encryption, the enabling mechanism being to deliver a decryption key and optionally a decryption algorithm.
   b) Missing parts, the enabling mechanism being to deliver the missing parts.

8. A method in accordance with any of the previous claims wherein the disabled media and other components of the invention are distributed to the client in the form of randomly accessible media files or as streams through:
   a) An installation process.
   b) A network file store.
   c) On an as needed basis through a network as in a thin client.

9. A method in accordance with any of the previous claims wherein the enabling mechanism is provided only after the client has been authenticated by means of a username, password, certificate, key, ip address, machine characteristics or other means.

10. A method in accordance with any of the previous claims wherein one or more of the the network communications is secured through encryption, a private network or other means.

11. A method in accordance with any of the previous claims further characterised by the use of 3 logical components as part of the main client side media enabling process:
    a) A Client Log-in Component (CLC) that contacts a networked machine and sends any initial authentication information from the client to that networked machine.
    b) A Check Module which is returned from a networked machine in response to valid client authentication information and is run by the client to validate the secured components the client has access to.
    c) A Client Instantiation Component (CIC) which allows the use of enabled media. The CIC may optionally return the Check Module results to the networked machine for validation itself and may receive and apply the enabling mechanism to the disabled media directly.

12. A method in accordance with claim 11 wherein the functions of the logical components are implemented in any of:
    a) Separate modules.
    b) Combined functionality modules or subroutines.
    c) Functional modules combined with disabled media parts.

13. A method in accordance with claims 11 or 12 wherein the process of enabling the media is characterised with reference to the figures by:
    a) The CLC contacting a networked machine with optional initial authentication information and receiving back a selected Check Module.

b) The Check Module executing and optionally validating components accessible by the client that should be secured in order to ensure the security of the enabling mechanism and the media.

c) The CIC being started in a preferably non-debug secured environment and any Check Results being returned to a networked machine (either by the CIC or another mechanism).

d) The CIC obtaining the enabling mechanism for the media from a networked machine.

e) The CIC enabling the use of portions of the media.

14. A method in accordance with claims 11, 12 or 13 wherein said networked machine is a Licence Management Service (LMS) with the following functionality:

a) Authenticates client CLC requests and returns selected Check Modules to the client.

b) Verifies Check Module results with reference to optional Check Module identification information and an optional time limit for the return of verification information.

c) Issues media enabling mechanisms to verified clients.

d) Optionally tracks usage and highlights potential license breaches by using machine and timing heuristics, log-in information and Check Module results.

15. A method in accordance with claim 14 wherein the LMS is distributed either functionally or on a load basis amongst several machines in a communications network or otherwise.

16. A method in accordance with any of the previous claims wherein the media is further defined to include: instantiable random access media such as software, sequential media such as films and music and other media such as books, application files, user work and data.

17. A method in accordance with claim 16 wherein the media includes Java application software.

18. A method in accordance with any of the previous claims wherein the process by which the enabled media is used is itself secure, characterised by one or more of:

a) Instantiating enabled software media either in the process space of the CIC or in a separate process space.

b) Providing enabled media parts to a, preferably secured, viewing application on a stream or a secured virtual file system basis.

c) The CIC using the enabled media.

19. A method in accordance with any of the previous claims wherein a different key or disabling mechanism is used for different media collections, files, users, clients or other units.

20. A method in accordance with any of the previous claims wherein the use of more than one disabled media collection is enabled by using shared enabling components such as shared CLC and CIC components.

21. A method substantially as herein described with reference to Figures 1 to 4 of the accompanying drawings.

22. Apparatus configured to perform any of the methods of the previous claims.

23. Use of any of the previous methods of claims.